Position: **Master IA/Security Specialist,** (Embedded Cyber Security Services)

Education: B.S. in a Computer Information Systems or related Degree Program (6 years relevant experience may be substituted for degree)

Job Description:
The IA/Security Specialist shall provide Cyber Security embedded (Program Office, lab etc.) services including the management of Information Systems Security Management services, including managing the IAVM program, managing compliance with CTO tasking, and managing the Cyber Security Workforce Management (CSM) program. He or she will also manage the Cyber Security Planning program. He or she will ensure that a detailed Cyber Security Program Plan is developed and executed based on a detailed analysis of the program mission coupled with current published DOD/DON/NAVAIR Cyber Security directives, instructions and processes. He or she shall provide an Integrated Master Schedule (CDRL A004) that outlines Cyber Security tasks and milestones that will be maintained as an overlay to program objectives communicated by the Program Manager.

Responsibilities:
- Supporting the Cyber Security Workforce Manager (CSM) and/or Command ISSM in the training and education of the NAVAIR Cyber Security Workforce (CSWF).
- Support the Command ISSM Manager by supporting command Cyber Security workforce training events and providing the Command ISSM with subject matter expertise in support of government-generated training materials, briefings and guides.
- Tracking training/certification requirements and communication with CSWF personnel.
- Performing the dissemination, collection, and reporting of DOD IAVM patching via Vulnerability Remediation Asset Manager (VRAM), or other Navy approved method.
- Performing the analysis, dissemination, collection, and reporting of CTO tasking via approved methods.
- Providing support in the administration and/or execution of new tasking as defined in CTO guidance including:
  - Public Key Infrastructure (PKI)
  - Data at Rest
  - Security Technical Implementation Guides (STIG)
  - HBSS policy
  - Security boundary architecture
- Ensuring that a detailed Cyber Security Program Plan is developed and executed based on a detailed analysis of the program mission coupled with current published DOD/DON/NAVAIR Cyber Security directives, instructions and processes.
- Providing an Integrated Master Schedule (CDRL A004) that outlines Cyber Security tasks and milestones that will be maintained as an overlay to program objectives communicated by the Program Office.

Qualifications:
- 10+ years of experience in a related IT field, and at least 5 years in a leadership role.
- DoD 8570 IAM III: CAP, CISSP, CISM, or GSLC certification
- B.S. in a Computer Information Systems or related Degree Program (6 years relevant experience may be substituted for degree)
- Secret Clearance with SSBI or TS/SCI with SSBI